UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/733,537	12/07/2000	Philip R. Graham	CSCO-86861	1789

7590 02/09/2004

WAGNER, MURABITO & HAO LLP
Third Floor
Two North Market Street
San Jose, CA 95113

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	6

DATE MAILED: 02/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/733,537	Applicant(s) GRAHAM, PHILIP R.	
	Examiner Brandon Hoffman	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 January 2004* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 December 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

1. Claims 1-20 are pending in this office action, claims 14-20 are newly added.

2. Applicant's arguments, see page 8 and 9, filed January 9, 2004, with respect to the rejection(s) of claim(s) 1-20 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Gupta et al. in view of Klebanoy et al., and further in view of Gibbs et al.

Rejections

3. The text of those sections of Title 35, U.S. Code not included in this office action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

4. Claims 1, 2, 5, 7-10, 12, and 14-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta et al. (U.S. Patent No. 6,389,532) in view of Klebanoy et al. (U.S. Patent No. 6,606,450).

Regarding claim 1, Gupta et al. teaches a digital signature method for a network infrastructure copy protection system (fig. 1), comprising:

- Applying a digital signature to a digital content file (col. 3, line 41-48);

- Transmitting the content file across a distributed computer network (col. 3, lines 49 and 50);
- Examining the content file to determine whether the content file includes the digital signature, the examining performed within the distributed computer network (col. 3, lines 50-54);
- Transmitting the content file when the content file includes the digital signature (col. 4, lines 7-11).
- Blocking transmission of the content file when the content file does not include the digital signature (col. 4, lines 12 and 13).

Gupta et al. does not teach blocking transmission of the content file when the content file comprises a restricted data format.

Klebanov et al. teaches blocking transmission of the content file when the content file comprises a restricted data format (fig. 3, ref. num 74 and 78).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine blocking transmission of the content file when the content file comprises a restricted data format, as taught by Klebanov et al., to the digital signature method of Gupta et al. It would have been obvious to combine blocking transmission of the content file when the content file comprises a restricted data format,

as taught by Klebanoy et al., to the digital signature method of Gupta et al. because blocking the restricted data type will prevent illegal copying of data.

Regarding claims 7 and 17, Gupta et al. teaches a restricted data format method for a network infrastructure copy protection system, comprising:

- Receiving a digital content file for transmission across a distributed computer network (fig. 7, ref. num 702); and
- Examining the content file, the examining performed within the distributed computer network (fig. 7, ref. num 704 and 706).

Gupta et al. does not teach examining the content file to determine whether the content file includes a restricted data format. Gupta et al. also does not teach transmitting the data file if the content file does not include the restricted data format, and blocking the file if the content filed does include the restricted data format.

Klebanoy et al. teaches examining the content file to determine whether the content file includes a restricted data format (fig. 3, ref. num 74), transmitting the data file if the content file does not include the restricted data format (fig. 3, ref. num 76), and blocking the file if the content filed does include the restricted data format (fig. 3, ref. num 78).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine examining the content file to determine whether the content file includes a restricted data format, transmitting the data file if the content file does not include the restricted data format, and blocking the file if the content filed does include the restricted data format, as taught by Klebanoy et al., to the restricted data format method of Gupta et al. It would have been obvious to combine examining the content file to determine whether the content file includes a restricted data format, transmitting the data file if the content file does not include the restricted data format, and blocking the file if the content filed does include the restricted data format, as taught by Klebanoy et al., to the restricted data format method of Gupta et al. because examining the content file and transmitting based on the lack of the restricted data format or blocking based on the presence of the restricted data format will prevent illegal copying of enriched data.

Regarding claim 2, the combination of Gupta et al. in view of Klebanoy et al. teaches the digital signature is configured to identify the sender of the digital content file (see col. 3, lines 44-46 of Gupta et al.).

Regarding claims 5 and 12, the combination of Gupta et al. in view of Klebanoy et al. teaches the examining is performed by a plurality of routers within the distributed computer network (see fig. 1, ref. num 104 of Gupta et al.).

Regarding claims 8-10, 14-16, 18, and 19, the combination of Gupta et al. in view of Klebanoy et al. teaches:

- The restricted data format is an MP3 data format (see col. 2, lines 10-13 of Klebanoy et al.);
- The restricted data format is an MPEG video data format (see col. 2, lines 10-13 of Klebanoy et al.); and
- The restricted data format is a Word document format (see col. 2, lines 10-13 of Klebanoy et al.).

Although the combination of Gupta et al. in view of Klebanoy et al. teaches the restriction of MPEG video data, it is well known in the art, that MP3 data, MPEG data, and Word document data are all enriched content that users transmit (illegally) through distributed networks, such as the Internet. It would have been obvious to apply the teachings of the combination of Gupta et al. in view of Klebanoy et al. to include MP3 data and Word document data, and any other data format deemed necessary to prevent illegal copying.

Regarding claim 20, the combination of Gupta et al. in view of Klebanoy et al. teaches further comprising examining the file to determine whether the file includes a valid digital signature (see col. 3, lines 50-54 of Gupta et al.).

Claims 3, 4, 6, 11, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Gupta et al. (U.S. Patent No. 6,389,532) in view of Klebanoy et al. (U.S. Patent No. 6,606,450), and further in view of Gibbs et al. (U.S. Patent No. 6,085,321).

Regarding claim 3, the combination of Gupta et al. in view of Klebanoy et al. teaches all of the subject matter of claim 1, as discussed above. However, the combination of Gupta et al. in view of Klebanoy et al. does not disclose the step of logging the digital signature applied to the content file within the distributed computer network when the content file is transmitted across the distributed computer network.

Gibbs et al. teaches the step of logging the digital signature applied to the content file within the distributed computer network when the content file is transmitted across the distributed computer network (fig. 4, ref. num 432 and col. 6, lines 17-26).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the step of logging the digital signature applied to the content file within the distributed computer network when the content file is transmitted across the distributed computer network, as taught by Gibbs et al., to the digital signature method of Gupta et al. in view of Klebanoy et al. It would have been obvious to combine the step of logging the digital signature applied to the content file within the distributed computer network when the content file is transmitted across the distributed

computer network, as taught by Gibbs et al., to the digital signature method of Gupta et al. in view of Klebanoy et al. because the step of logging the digital signature applied to the content file within the distributed computer network when the content file is transmitted across the distributed computer network would keep track of the status information and other information about the creation and authentication of digital signatures (see col. 3, lines 63-66 of Gibbs et al.).

Regarding claims 4 and 11, the combination of Gupta et al. in view of Klebanoy et al. teaches all of the subject matter of claims 1 and 7, respectively, as discussed above. However, the combination of Gupta et al. in view of Klebanoy et al. does not disclose the distributed computer network is the Internet.

Gibbs et al. teaches the distributed computer network is the Internet (fig. 4, ref. num 444).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to use the Internet as the distributed computer network, as taught by Gibbs et al., with the methods of Gupta et al. in view of Klebanoy et al. It would have been obvious to use the Internet as the distributed computer network, as taught by Gibbs et al., with the methods of Gupta et al. in view of Klebanoy et al. because using the Internet as the distributed computer network would allow the secure network of Gupta et al. to expand its security to a larger group of people and computers.

Regarding claims 6 and 13, the combination of Gupta et al. in view of Klebanoy et al. teaches all of the subject matter of claims 1 and 7, respectively, as discussed above. However, the combination of Gupta et al. in view of Klebanoy et al. does not disclose the examining is performed by a plurality of cache engines within the distributed computer network.

Gibbs et al. teaches the examining is performed by a plurality of cache engines within the distributed computer network (fig. 4, ref. num 420 and col. 7, lines 13-28).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to use a plurality of cache engines to perform the examining within the distributed computer network, as taught by Gibbs et al., with the methods of Gupta et al. in view of Klebanoy et al. It would have been obvious to use a plurality of cache engines to perform the examining within the distributed computer network, as taught by Gibbs et al., with the methods of Gupta et al. in view of Klebanoy et al. because the use of a plurality of cache engines to perform examining within the distributed computer network would allow faster examining of data as it is passed over the distributed computer network (see col. 7, lines 15-25 of Gibbs et al.).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon Hoffman whose telephone number is 703-305-4662. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Brenda Hoff

BH
2/2/04

Ayaz Sheikh

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100